REMARKS

I. Introduction

In response to the Office Action dated October 9, 2003, claims 3, 6, and 18 have been amended. Claims 1-23 remain in the application. Re-examination and re-consideration of the application, as amended, is requested.

II. Claim Amendments

Applicants' attorney has made amendments to the claims as indicated above. These amendments were made solely for the purpose of clarifying the language of the claims, and were not required for purposes of patentability.

III. The Cited References and the Subject Invention

A. The Rallis Reference

U.S. Patent No. 6,216,230, issued April 10, 2001 to Rallis et al. discloses a notebook security system (NBS) that prevents unauthorized use of a computer. A program resident on the computer and implements a user-validation procedure. A key device carries a first serial number and an encryption key. A second serial number is stored in said computer, the second serial number being the serial number of a device internal to the computer. A mass storage device installed in said computer stores a validation record. The validation record comprises an unencrypted portion and an encrypted portion, the unencrypted portion including a copy of said first serial number and said encrypted portion including a copy of said second serial number and a user personal identification number. The key device is interfaced to the computer. The first serial number and the encryption key are read from said key device in order to gain authorized use of said computer. The key device may be removed from the computer after authorized use of the computer has been gained, and during operation of the computer.

B. The Subject Invention

The Applicants' invention is a method and apparatus for securing a token from unauthorized use. The method comprises the steps of receiving a first message transmitted from a host processing device and addressed to a PIN entry device according to a universal

serial bus (USB) protocol; accepting a PIN entered into the PIN entry device; and transmitting a second message comprising at least a portion of the first message and the PIN from the PIN entry device to the token along a secure communication path. In another embodiment, the present invention describes an apparatus for securing a token from unauthorized use, comprising a PIN entry device, communicably coupleable to a host processing device transmitting a first message addressed to the PIN entry device, and communicatively coupleable to the token according to a universal serial bus USB protocol, the PIN entry device comprising a user input device, for accepting a user-input PIN; and a processor, communicatively coupled to the user input device, the processor for receiving the first message and combining the first message with the user-input PIN, and for producing a second message having at least a portion of the first message and the user-input PIN.

C. Differences Between the Subject Invention and the Cited References

The Rallis reference does not discloses a system for securing a token from unauthorized use. Instead, Rallis teaches the use of a token to prevent unauthorized use of a notebook computer. To achieve this aim, the Rallis reference discloses a system wherein the PIN is entered by a conventional keyboard coupled to a host computer, not by a device coupled between a token and the host computer, as described in the Applicants' invention. Rallis also does not disclose intercepting PIN commands from the host computer ... in fact, no message having a PIN is ever sent to the key. The only message sent to the key is a "super key" which is stored in the computer (BIOS), not something that the user entered. With the foregoing in mind, the Examiner is invited to consider the following remarks.

IV. Office Action Prior Art Rejections

In paragraphs (1)-(2), the Office Action rejected claims 1-23 under 35 U.S.C. § 102(e) as anticipated by Rallis et al., U.S. Patent No. 6,216,230 (Rallis). Applicants respectfully traverse these rejections. The Applicants respectfully traverse these rejections.

With Respect to Claims 1 and 12: Claim 1 recites:

> *A method of securing a token from unauthorized use, comprising the steps of:*
> *receiving a first message transmitted from a host processing device and addressed to a PIN entry device according to a universal serial bus (USB) protocol;*
> *accepting a PIN entered into the PIN entry device; and*

transmitting a second message comprising at least a portion of the first message and the PIN from the PIN entry device to the token along a secure communication path.

According to the Office Action, Rallis discloses a method of securing a token from unauthorized use as follows:

> A program running on the notebook computer 10 uses the key device serial number and the encryption key, along with a Personal Identification Number (PIN), in a user-validation procedure to prevent operation (i.e. power-up) of the note book computer 10 by an unauthorized user. For maximum security protection, the key device 20 is connected only during the user-validation procedure and is carried and stored separately from the notebook computer 10. (col. 2, lines 52-56)

However, the Rallis reference is not directed to a system preventing unauthorized use of a token, but rather, a system that uses a token to prevent unauthorized use of a computer. On this basis alone, the rejection under 35 U.S.C. 102(e) is improper and should be withdrawn.

The Office Action also indicates that the Rallis reference discloses the step of *"receiving a first message transmitted from a host processing device and addressed to a PIN entry device according to a universal serial bus (USB) protocol"* as follows:

> A program that is automatically invoked at computer power-up, or reset, implements the user-validation procedure. The user is prompted to connect the key device to the computer. In the preferred embodiment, the user is prompted to enter a PIN, although the system can be configured to operate without manual PIN entry. (col. 1, lines 49-54)

The Applicants respectfully disagree. The foregoing teaches that the user connects and key to the notebook computer and enters a PIN into the notebook computer. Accordingly, there is no "PIN entry device" except perhaps the "notebook computer" which cannot be connected to itself via a USB protocol.

The Office Action also indicates that the Rallis reference discloses the step of *"transmitting a second message comprising at least a portion of the first message and the PIN from the PIN entry device to the token along a secure communication path"* as follows:

> The procedure permits entry past a first security level only if the key device serial number matches the unencrypted numbers in the validation record. If the first-level validation is successful, the procedure then uses the encryption key to decrypt the hard drive serial number and PIN found in the stored validation record. (col. 1, lines 54-59)

Of course, the foregoing does not disclose transmitting a second message comprising a PN from a PIN entry device to a token. Rallis teaches a system wherein the PIN is entered into the notebook computer and used for further processing. It is not transmitted anywhere,

let alone via from a PIN entry device to a token. Accordingly, the Applicants respectfully traverse the rejection of claim 1.

Claim 12 recites

> *a PIN entry device, communicably coupleable to a host processing device transmitting a first message addressed to the PIN entry device, and communicatively coupleable to the token according to a universal serial bus USB protocol, the PIN entry device comprising:*
>
> *a user input device, for accepting a user-input PIN; and*
>
> *a processor, communicatively coupled to the user input device, the processor for receiving the first message and combining the first message with the user-input PIN, and for producing a second message having at least a portion of the first message and the user-input PIN*

As discussed above, Rallis does not disclose a PIN entry device communicatively coupled to a host processing device and to a token according to a USB protocol. Nor does Rallis disclose a PIN entry device having a processor that receives the first message and combines it with a user-entered PIN to produce a second message. Accordingly, the rejection of claim 12 is traversed as well.

With Respect to Claim 2: Claim 2 recites that the first message received in the PIN entry device and the second message is transmitted from the PIN entry device directly to the token along the secure communication path. According to the Office Action, these features are disclosed as follows:

> The user is prompted to connect the key device to the computer. In the preferred embodiment, the user is prompted to enter a PIN, although the system can be configured to operate without manual PIN entry. (col. 1, lines 51-54)

and at

> The procedure permits entry past the second security level only if the validation record is properly decrypted, the installed hard disk serial number matches the decrypted number, and the manually-entered PIN matches the decrypted PIN. A failure at any step in the user-validation procedure will immediately power down the computer, thereby rendering it useless to a thief not possessing the required key device. (col. 1, lines 60-67)

and

> A program running on the notebook computer 10 uses the key device serial number and the encryption key, along with a Personal Identification Number (PIN), in a user-validation procedure to prevent operation (i.e. power-up) of the note book computer 10 by an unauthorized user. For maximum security protection, the key device 20 is connected only during the user-validation procedure and is carried and stored separately from the notebook computer 10. (col. 2, lines 52-56)

As described above with respect to claim 1, the Rallis reference does not teach transmitting a PIN anywhere via a USB protocol. Accordingly, the rejection of claim 2 is traversed as well.

With Respect to Claim 3: Claim 3 recites that the step of receiving the first message from the host processing device and addressed to a PIN entry device comprises the steps of:

> *receiving the first message in a USB-compliant hub communicatively coupled to the host processing device via a first communication path; and*
> *transmitting the first message to the PIN entry device communicatively coupled to the USB-compliant hub*

and that the step of transmitting the second message comprising a portion of the first message and the PIN and at least a portion of the first message from the PIN entry device to the token along a secure communication path comprises the steps of:

> *transmitting a second message from the PIN entry device via the USB hub.*

The Office Action indicates that the step of receiving the first message transmitted from a host processing device and addressed to a PIN entry device is disclosed as follows:

> The procedure permits entry past a first security level only if the key device serial number matches the unencrypted numbers in the validation record. If the first-level validation is successful, the procedure then uses the encryption key to decrypt the hard drive serial number and PIN found in the stored validation record. (col. 1, lines 54-59)

Plainly, the foregoing does not disclose a USB-compliant hub at all, let alone the other features of claim 1. The Office Action therefore argues that a hub is "inherently disclosed" because Rallis discloses a USB port 14. However, a USB port is not a USB hub, and inherency "may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient." *Continental Can Co. v. Monsanto Co.*, 948 F.2d 1264, 1269(Fed. Cir. 1991). Instead, to establish inherency, the extrinsic evidence "must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill." *Continental Can Co.*, 948 F.2d at 1268.

There is nothing about the Rallis reference that indicates that a USB hub is "necessarily present". Indeed, the Rallis system has no need whatsoever for a USB hub.

The Office Action includes further reference to other portions of the Rallis reference, but these portions do not disclose a USB hub, nor do they provide evidence supporting an argument that a USB hub is necessarily present in the Rallis device. Accordingly, the Applicants respectfully traverse the rejection of claim 3.

With Respect to Claim 4: Claim 4 recites that the step of transmitting the second message from the PIN entry device via the USB-compliant hub comprises the steps of:

> *transmitting a third message comprising the PIN from the PIN entry device to the USB-compliant hub;*
>
> *processing the message in the USB-compliant hub to produce the second message; and*
>
> *transmitting the second message from the USB-compliant hub.*

According to the Office Action, the foregoing steps are disclosed as follows:

> A program that is automatically invoked at computer power-up, or reset, implements the user-validation procedure. The user is prompted to connect the key device to the computer. In the preferred embodiment, the user is prompted to enter a PIN, although the system can be configured to operate without manual PIN entry. The procedure permits entry past a first security level only if the key device serial number matches the unencrypted numbers in the validation record. If the first-level validation is successful, the procedure then uses the encryption key to decrypt the hard drive serial number and PIN found in the stored validation record. The procedure permits entry past the second security level only if the validation record is properly decrypted, the installed hard disk serial number matches the decrypted number, and the manually-entered PIN matches the decrypted PIN. A failure at any step in the user-validation procedure will immediately power down the computer, thereby rendering it useless to a thief not possessing the required key device. (col. 1, lines 49-67).

The Applicants respectfully disagree. Nothing in the foregoing text discloses transmitting a third message comprising the PIN from the PIN entry device to a USB-compliant hub, processing the message in the hub to produce a second message, or transmitting the second message from the USB-compliant hub. Rallis fails to discloses a hub and teaches that the PIN is accepted in the notebook computer and is not transmitted anywhere else. Accordingly, the Applicants respectfully traverse the rejection of claim 4 as well.

With Respect to Claim 5: Claim 5 recites that the signal received from the host processing device is generated in an API interface. The Office Action argues that this is inherently disclosed in Rallis, because Rallis discloses messages that are both sent to and received by the token and the notebook.

Inherency "may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient." *Continental Can Co. v. Monsanto Co.*, 948 F.2d 1264, 1269(Fed. Cir. 1991). Instead, to establish inherency,

the extrinsic evidence "must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill." *Continental Can Co.*, 948 F.2d at 1268. The Applicants traverse this rejection, because messages can be sent from different devices without resort to an API interface, and hence, the "inherency doctrine" is not applicable here.

With Respect to Claims 6, 8, 9, 13, and 15: Claim 6 recites that the first that the first message is encrypted according to a first encryption key, and that the entry device comprises a decryption module having access to the first encryption key for decoding the first message. The Office Action indicates that this is disclosed as follows:

> Briefly, a security system constructed in accordance with the invention implements a user-validation procedure that requires the user to connect the proper hardware "key" device to a computer at power-up to enable operation. The system can support multiple users and a single supervisor. Each authorized user is provided with a unique key device which is carried and stored separately from the computer. The key device holds a unique serial number and an encryption key. A validation record stored on the computer's hard disk contains an unencrypted key device serial number, an encrypted hard disk serial number, and a Personal Identification Number (PIN) unique to the user.
>
> A program that is automatically invoked at computer power-up, or reset, implements the user-validation procedure. The user is prompted to connect the key device to the computer. In the preferred embodiment, the user is prompted to enter a PIN, although the system can be configured to operate without manual PIN entry. The procedure permits entry past a first security level only if the key device serial number matches the unencrypted numbers in the validation record. If the first-level validation is successful, the procedure then uses the encryption key to decrypt the hard drive serial number and PIN found in the stored validation record. The procedure permits entry past the second security level only if the validation record is properly decrypted, the installed hard disk serial number matches the decrypted number, and the manually-entered PIN matches the decrypted PIN. A failure at any step in the user-validation procedure will immediately power down the computer, thereby rendering it useless to a thief not possessing the required key device. (col. 1, lines 37-67)

However, the foregoing does not teach a PIN entry device having a decryption module for decoding the first message. The Rallis reference teaches that the PIN is entered directly into the notebook computer. Since Rallis teaches that the PIN is not transmitted from the host computer anywhere else, it is not subject to compromise, and hence, there is no reason whatever to encrypt the PIN and decrypt it with a decryption module. Claim 13 is allowable for the same reasons. Claims 8 and 15 likewise recite decryption modules that are not needed or employed in Rallis. Accordingly, the Applicants respectfully traverse the rejection of claims 6, 8, 9, 13, and 15.

With Respect to Claims 10 and 11: Claim 10 recites that the first message is a message transmitted from the host processing device to authorize a transaction, and claim 11 recites that the first message is a message transmitted from the host processing device to

authenticate a user of the token. According to the Office Action, these features are disclosed as follows:

> A program that is automatically invoked at computer power-up, or reset, implements the user-validation procedure. (col. 1, lines 49-51)

and

> FIG. 2 is a block diagram of the major components within the Central Processing Unit (CPU) 50 address space for a conventional IBM PC-compatible computer. At power-up, the CPU 50 accesses the Basic Input/Output System (BIOS) Read-Only Memory (ROM) 30 and executes a "boot-up" procedure. Prior to the termination of the bootup procedure, the CPU downloads the operating system (OS) program via a memory-mapped interface 40 from a mass storage device, such as a hard drive 42 or possibly a diskette 44, and reads it into main Random-Access Memory (RAM) memory 60. In the preferred embodiment of the invention, the boot-up user-validation program resides in a ROM adapter 34 of the BIOS 30 and is executed at boot-up and prior to the download of the operating system. (col. 2, line 61 through col. 3, line 7)

None of the foregoing refers to a "transaction", and Rallis does not authenticate the user of a token. Rallis is directed to using a token to unlock a notebook computer. The Applicants therefore traverse these rejections as well.

With Respect to Claim 18: Claim 18 recites:

> *A method for securing a token from unauthorized use, comprising:*
> *intercepting a first message from the host processing device addressed to the token in a hub;*
> *providing the intercepted message to a PIN entry device communicatively coupled to the hub;*
> *accepting a second message from the PIN entry device comprising a user-entered PIN;*
> *generating a third message from the second message, the third message comprising the user-entered PIN and at least a portion of the first message; and*
> *transmitting the third message from the USB-compliant hub to the token.*

According to the Office Action, the limitations of claim 18 were already discussed in the rejections of claims 1 and 3-4, but this is not the case. Nothing in Rallis discloses intercepting a message from a host processing device addressed to the token in a hub. Rallis, in fact, fails to disclose intercepting any message, fails to disclose sending a message from a host processing device to a token, and fails to disclose a hub at all. The Office Action does not indicate which messages are the "second" and "third" messages described in the claim, and the Applicants can ascertain no such disclosure. Accordingly, the Applicants traverse the rejection of claim 18.

With Respect to Claim 20: Claim 20 recites:

a USB-compliant hub, communicably coupleable between a host processing device and the token, the USB compliant hub having;

means for intercepting a message addressed to the PIN entry device;

means for generating a third message from the first message and a user-entered PIN; and

means for transmitting the third message to the token;

a PIN entry device, communicatively coupled to USB-compliant hub, for accepting a user-entered PIN and providing the user-entered PIN to the USB-compliant hub.

The Office Action asserts that Rallis inherently discloses a USB-compliant hub, because it discloses a USB-compliant port. However, a USB hub is not analogous to a USB port, and nothing in the Rallis reference indicates that a USB hub is necessarily present. Rallis likewise fails to disclose a PIN entry device. For these reasons and the others described above, claim 20 is allowable over the Rallis reference.

With Respect to Claim 21: As discussed above, Rallis does not disclose a means for intercepting a message to a PIN entry device or for generating the messages recited in claim 21. Accordingly, the rejection of claim 21 is traversed as well.

With Respect to Claim 22 and 23: As discussed above with respect to claims 6, 8, 9, 13, and 15, Rallis does not disclose, nor does it have a need for, encryption modules in a PIN entry device. Accordingly, claims 22 and 23 are allowable as well.

V. Dependent Claims

Dependent claims 2-11, 13-17, 19, and 21-23 incorporate the limitations of their related independent claims, and are therefore patentable on this basis. In addition, these claims recite novel elements even more remote from the cited references. Accordingly, the Applicants respectfully request that these claims be allowed as well.

VI. Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

GATES & COOPER LLP
Attorneys for Applicant(s)

Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, California 90045
(310) 641-8797

Date: January 7, 2004

By: _____
Name: Victor G. Cooper
Reg. No.: 39,641

VGC/mrj